IN THE CLAIMS

Please amend the claims as follows:

1. (currently amended) A method ~~of~~ for processing communication traffic, said method comprising:

detecting an anomaly in ~~the~~ communication traffic within a communication network;

in response to a detection of an anomaly occurred in said communication traffic, applying a ~~first~~ blocking measure A, a blocking measure A & B, and a blocking measure A & !B to ~~the anomalous~~ said communication traffic for stopping said anomaly ~~that stops the anomalous traffic~~;

determining whether or not said anomaly reoccurs after said blocking measure A & B has been temporarily removed;

in response to a determination that said anomaly does not reoccur, canceling said block measure A & B from being applied to said communication traffic and enforcing said blocking measure A & !B on said communication traffic; and

in response to a determination that said anomaly reoccurs, reimposing said blocking measure A & B on said communication traffic and temporarily removing said blocking measure A & !B from said communication ~~determining a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous~~ traffic.

2. (currently amended) The method of Claim 1, wherein method further includes ~~determining the second blocking measure B comprises~~:

determining whether or not said anomaly reoccurs after said blocking measure A & !B had been temporarily removed;

in response to a determination that said anomaly does not reoccur, canceling said block measure A & !B from being applied to said communication traffic and enforcing said blocking measure A & B on said communication traffic ~~applying a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B)~~; and

in response to a determination that said anomaly reoccurs, reimposing said block measure A on said communication ~~enforcing the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous~~ traffic.

3. (currently amended) The method of Claim ~~2~~ 1, wherein said blocking measure A & !B is a less restrictive blocking measure than said blocking measure A & B ~~further comprising: determining a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic~~.

4. (currently amended) The method of Claim ~~2~~ 1, wherein said detecting further includes detecting a pattern in a value of at least one protocol field associated with said communication ~~determining the second blocking measure B further comprises:~~

~~applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and~~

~~enforcing the logical combination (A & B) if the logical combination (A & B) stops the anomalous~~ traffic.

5. (currently amended) The method of Claim 4 1, wherein said detecting further includes detecting whether or not a flow rate of said anomalous traffic has exceeded a predetermined threshold ~~comprising:~~

~~determining a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) stops the anomalous traffic.~~

6-27. canceled.

28. (new) A computer readable medium having a computer program product for processing communication traffic, said computer readable medium comprising:

computer program code for detecting an anomaly in communication traffic within a communication network;

computer program code for, in response to a detection of an anomaly occurred in said communication traffic, applying a blocking measure A, a blocking measure A & B, and a blocking measure A & !B to said communication traffic for stopping said anomaly;

computer program code for determining whether or not said anomaly reoccurs after said blocking measure A & B has been temporarily removed;

computer program code for, in response to a determination that said anomaly does not reoccur, canceling said block measure A & B from being applied to said communication traffic and enforcing said blocking measure A & !B on said communication traffic; and

computer program code for, in response to a determination that said anomaly reoccurs, reimposing said blocking measure A & B on said communication traffic and temporarily removing said blocking measure A & !B from said communication traffic.

29. (new) The computer readable medium of Claim 28, wherein computer readable medium further includes:

computer program code for determining whether or not said anomaly reoccurs after said blocking measure A & !B had been temporarily removed;

computer program code for, in response to a determination that said anomaly does not reoccur, canceling said block measure A & !B from being applied to said communication traffic and enforcing said blocking measure A & B on said communication traffic; and

computer program code for, in response to a determination that said anomaly reoccurs, reimposing said block measure A on said communication traffic.

30. (new) The computer readable medium of Claim 28, wherein said blocking measure A & !B is a less restrictive blocking measure than said blocking measure A & B.

31. (new) The computer readable medium of Claim 28, wherein said computer program code for detecting further includes computer program code for detecting a pattern in a value of at least one protocol field associated with said communication traffic.

32. (new) The computer readable medium of Claim 28, wherein said computer program code for detecting further includes computer program code for detecting whether or not a flow rate of said anomalous traffic has exceeded a predetermined threshold.